Description

Security module for encrypting a telephone conversation

The invention relates to a security module for encrypting a telephone conversation between one or more first telecommunication terminals in a packet-oriented data network and one or more second telecommunication terminals in an analog and/or digital telephone network.

Telephony in IP networks is known from the prior art. Standards now exist in which the signaling for telephony in IP-networks is defined. The standards concerned here are the IETF Standard SIP and the ITU Standard H.323, which is also referred to as "Voice over IP" (VoIP) and is mainly employed in LAN or WLAN-based networks (LAN = Local Area Network, WLAN Wireless Local Area Network). With VoIP telephony security aspects have been mainly considered to date in relation to the authenticity and Integrity of control and signaling data. In future solutions, in addition to the pure signaling security, the security of the transferred voice data will also be considered. To secure voice data in IP networks for example the encrypted transport protocol SRTP (SRTP = Secure Real Time Transport Protocol; see document [1]) comes into consideration.

With the current security solutions however only security of voice data in packet-oriented networks is guaranteed. Although security solutions also exist for telephony in public telephone networks, however there has not been an opportunity thus far for conducting encrypted telephone conversations from a packet-oriented network to a public telephone network.

The object of the invention is therefore to create a security module for encrypting a telephone conversation which enables encryption of the voice data in a heterogeneous network comprising a packet-oriented data network and a telephone network.

This object is achieved by the independent claims. Developments of the invention are defined in the dependent claims.

The inventive security module serves to encrypt a telephone conversation between one or more first telecommunication terminals in a packet-oriented data network and one or more second telecommunication terminals in an analog and/or digital telephone network, with data packets being transported by means of an encrypted transport protocol in the packet-oriented network and the keys for the encrypted transport protocol being exchanged by means of a key exchange protocol. A telephone network is taken below to be any type of PSTN (PSTN = Public Switched Telephone Network) which means that both an analog and also a digital telephone network can be involved. The packet-oriented network and the telephone network in this case are connected to each other via a gateway computer and the security module can be connected into a connecting line at a first or second telecommunication terminal for a telephone conversation. The term "connecting line" is in this case to be understood in general terms, which means that it can involve a wired and also a wireless connection at the corresponding telecommunication terminal.

The inventive security module comprises a protocol processing device which processes messages of the key exchange protocol as well as data packets transported by means of the encrypted transport protocol, if the security module is connected into a connecting line for a telephone conversation at a first or second telecommunication terminal. The task of the protocol processing device is to convert voice signals which are created at the corresponding telecommunication terminal into data packets for transport via the encrypted transport protocol and to convert incoming data packets at the security module which are transported via the encrypted transport protocol, into voice signals.

The security module further features a modem connection unit which is always used if the security module is connected into a connection line at a second telecommunication terminal. In this case the modem connection unit sets up a modem connection for a telephone conversation between the second telecommunication terminal and the gateway and/or a further second telecommunication terminal, with data packets being transported by means of the encrypted transport protocol as well as messages of the key exchange protocol over the modem connection. Preferably a PPP connection (PPP = Point-to-Point Protocol) runs over the modem connection with which the data packets of the transport protocol as well as messages of the key exchange protocol are transported. The modem connection unit in the security module thus implements a transfer of encryption technologies from packet-oriented networks into public telephone networks. This is possible since modem connections currently have sufficient bandwidth or transmission rates for transmitting real-time media data packets.

In an especially preferred embodiment SRTP is used as the encrypted transport protocol (see document [1]). The key exchange protocol MIKEY (= Multimedia Internet KEYing) is preferably used for the exchange of the keys which are used in the encrypted transport protocol MIKEY is currently a draft at the IETF which will be declared a standard in the foreseeable future.

In a further embodiment of the security module messages of the key exchange protocol are transported for a telephone conversation via the SIP (SIP = Session Initiation Protocol), with the protocol processing device of the security module being embodied such that it can process this protocol.

The telephone network in which the inventive security module is used is for example a digital ISDN network. Preferably the modem connection unit in this case sets up a modem connection via the B channel in the ISDN network. The packet-oriented network involved is preferably an IP-based data network, especially a LAN network. The modem connection unit preferably establishes a modem connection in accordance with the V90 and/or V92 standard, with this standard providing a sufficient bandwidth or transmission rates for transmitting data packets from packet-oriented networks.

In a variant of the invention the security module is used for telephones with a connecting cable between telephone and telephone handset, with the security module being embodied such that it can be connected into the connecting cable.

Exemplary embodiments of the invention are explained below with reference to the enclosed drawing.

The drawings show

Figure 1 the schematic diagram of a heterogeneous network in which the inventive security module for encryption of voice signals is used.

The heterogeneous network shown in Figure 1 on the one hand includes an IP-based LAN (LAN = Local Area Network) as well as a public TDM (TDM = Time Division Multiplexing) telephone network. The TDM network is a digital network, with a special analog speech channel being used however for transmission of spoken words. The LAN and the TDM network are connected to each other via a gateway G. The gateway is used to modify IP data packets transmitted in the LAN network for forwarding in the TDM network as well as data from the TDM network for forwarding in the LAN network in the appropriate manner.

There are two VoIP clients VoIP-C in the LAN network which make telephony via packet-oriented networks possible. The SIP or H.323 standards sufficiently well-known to the person skilled in the art can be used when telephoning via "Voice over IP”. The lower VoIP client in Fig. 1 is a telephone with which the intention is to set up an encrypted telephone call. Therefore the inventive security module is connected between the handset of the telephone and the actual telephone in the corresponding connecting line.

In the TDM network of Figure 1 for example two TDM clients, TDM-C, in the form of telephones are shown, with which encrypted telephone conversations can also be conducted. Therefore in these telephones too the inventive security module SM is also connected in the connecting line between the handsets and the actual telephone.

The security modules known from the prior art allow an encryption of the telephone call only within the TDM network, in which case each telephone caller, to set up an encrypted telephone call, creates a key in each case by pressing a button on his security module, with the keys then being exchanged via a proprietary signaling protocol between the telephones of the participants. Finally combinations of numbers are shown on the displays which are integrated into the security modules which the callers exchange with each other over the telephone connection If the combinations of numbers match it can be assumed that the call is not being overheard by any third party so that with the aid of the exchanged keys encrypted data transmissions is finally undertaken, with a proprietary protocol again being used here. Experiments have shown that with the conventional security modules no encrypted telephone conversations between a telephone in a packet-oriented network and a telephone in a TDM network can be conducted. The result is thus that in packet-oriented networks the data is transmitted asynchronously, which can lead to bandwidth variations (also known as jitter) which cannot be processed by conventional security modules. Likewise data packet losses arising in packet-oriented networks lead to problems with conventional security modules.

The security module in accordance with the embodiment described here solves this problem by being able to process the protocols known from the IP world for encrypting data in a normal public TDM network. To this end a protocol processing device is provided in the security module which can process the encrypted transport protocol SRTP (SRTP = Secure Real Time Protocol). This protocol is likely to become the future standard for encrypted transmission of media data. In addition the protocol processing device can process the key exchange protocol MIKEY. Keys are created with this protocol and exchanged between the clients or telephones in the heterogeneous network of Fig. 1. The keys in this case are used by the transport protocol SRTP for encrypted transmission of the data packets by means of SRTE. The protocol processing device enables facilities such as encrypted telephony between VoIP clients in the LAN network. This is shown in Figure 1 by the double arrows MIKEY-KM (KM stands for KEY Management) and SRTP-MS (MS stands for Media Security).

To set up an encrypted telephone call between subscribers in the TDM network or between a subscriber in the LAN network and a subscriber in the TDM network, the security module SM features a modem connection unit. This modem connection unit establishes a modem connection for a telephone conversation of a subscriber in the TDM network to a subscriber in the LAN network via a voice channel in the TDM network to the gateway G. Preferably this involves a V92 modem connection which can transmit the data at 56 kbit/s downstream and 48 kbit/s upstream. Via this connection a further connection is made available via the PPP (PPP = Point to Point Protocol), with data being transported via the latter in the key exchange protocol MIKEY or in the SRTP protocol. Since these protocols can be processed by the protocol processing device in the security module SM a migration of the protocols from the LAN network into the TDM network is thus made possible.

The MIKEY messages are transported in the LAN network for example via the SIP protocol. In the gateway the contents of the MIKEY messages can then be cut out of the SIP message and inserted into the PPP tunnel. It would however also be conceivable for the gateway to simply send the SIP messages onwards in the PPP tunnel, without cutting out the MIKEY messages. In such a case the protocol processing unit of the security module must be able to process the SIP protocol. Thus a solution is also conceivable in which the security module SM functions as an SIP end point. In relation to the data which is transported via the SRTP protocol, the gateway G only assumes a forwarding function and does not modify the data. This also applies to the actual key exchange data in the form of MIKEY messages. Where necessary the gateway can however also be included as a trustworthy component in the connection, in order to allow. "lawful interception" for example.

The arrows in the lower part of Figure 1 again illustrate the inventive mechanism. The double arrow labeled p-IP (p-IP = plain IP) highlights the fact that a purely IP-based encrypted data transmission is used between a VoIP-Client VoIP-C and the gateway G. By contrast a modem connection is used between the gateway G and a TDM client TDM-C for encrypted data transport via which the PPP protocol runs, with which IP data packets are again transported. This is indicated by the double arrow IP-PPP-TDM. Despite these different connection mechanisms, an end-to end encryption between a client in the LAN network and a client in the TDM network by means of the key exchange protocol MIKEY and of the SRTP transport protocol SRTP is obtained. This is highlighted by the double arrows labeled MIKEY-KM and SRTP-MS.

The transmission of encryption protocols known from the IP world in a public telephone network is thus made possible in a simple manner with the inventive security module. This is guaranteed by a modem connection which, as a result of the bandwidths or transmission rates now possible with such a connection, makes possible the transport of real time data packets and signaling messages from the IP world.

Literature references:

[1] Internet Draft: The Secure Real-time Transport Protocol; Baugher, McGrew, Oran, Blom, Carrara, Naslund, Norrman; Work in Progress; http://search.ietf.org/internetdrafts/draft-ietf-avt-srtp-09.txt

[2] Internet Draft: MIKEY: Multimedia Internet KEYing; J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman; Work in Progress; http://search.ietf.org/internetdrafts/draft-ietf-msec-mikey-07.txt